Date:03/02/2024

Assessment 2

Investigation of Data Breach

This assessment gives us complete understanding on **Investigation of Data Breach** by analyzing the **renowned organizations** which were already fall under **leakage of sensitive data**.

Objectives

Main objective of this project is to gain knowledge on **investigation of Data Breach and usage of forensic tools**.This project encourage us to learn more about data breach how the companies fall under data breaches and how they are overcoming from it.And to know **complete analysis of Data breach.**

Data Breach

A **Data Breach** is a security incident in which a **party gains unauthorized access to sensitive or confidential information**, including personal information (Social Security number, bank account, medical information) or company information (customer information, personal property, financial information). The terms “data breach” and “exfiltration” are often used interchangeably with “cyber attack.” Data breaches only include security breaches that result in a **breach of data privacy**. Physical theft of hard drives, flash drives, or even files containing sensitive information is also known as a data breach.

This contain some keypoints

- **How** Data Breaches happen
- **Why** Data Breaches happen
- **Prevention and Mitigations**
- **Tools** used for investigation

How Data Breaches happen

Hackers find a target and then look for vulnerabilities in the target’s computer or personnel.They will also purchases malware that gives them access to the target network by stealing data beforehand.After determining the target and method,the hacker initiates the attack.Hackers may launch a social media campaign, exploit a vulnerability directly on the target,use stolen credentials,or use other information to attack the attacker.Hackers find the information they need and work. This could mean stealing data for use or sale,destroying data,or using ransomware to freeze data.

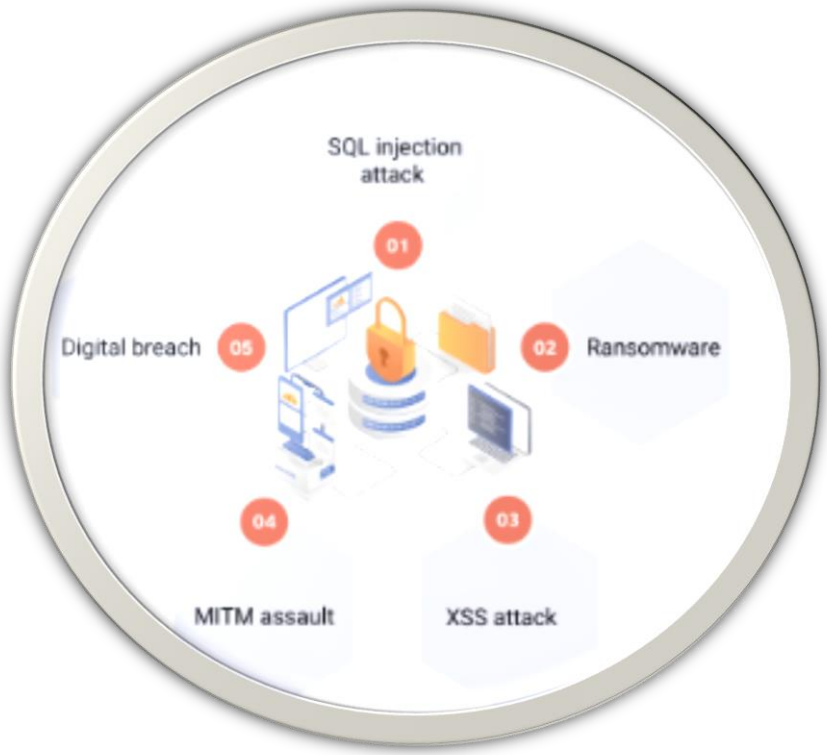

Fig1: Most attcks to DataBreach

Several ways to occur **Data Breach**

- Phishing Attacks
- Malware
- Weak Passwords
- Insider Threats
- Physical Theft
- Unpatched Software
- SQL Injection
- Man-in-the-Middle Attacks
- Social Engineering
- Third-Party Vulnerabilities

74 percent of **crimes** involved **a human element;** It was committed through **er rors, abuse, use** of stolen **credentials,** or **social engineering.83%** of **crimes** in volve other actors,the main motivation for attack is still financial and accounts f or **95%** of crimes. Thse three main ways **attackers gain access** to organizations are **credential theft, phishing,** and **exploits.**

Why Data Breaches happen

Innocentmistakes,Maliciousinsiders

HackersMost **malicious attacks** are for **financial gain**. Hackers can steal credit card numbers, bank accounts or other financial information to **steal money** dire ctly from **individuals** and **companies**. They may steal personally identifiable in formation(PII)—Social Security numbers and phone numbers for identity theft (to obtain loans and open credit cards in the victim's name) or s ell them on the dark web. Unauthorized organizations may steal competitors' tra de secrets. National actors may disrupt government systems to steal information relevant to political, military, or national development. Some violations are co mpletely devastating; hackers access **sensitive data** only to **damage** or **destroy** it, and hacktivist groups seek to **disrupt the organization.**

Prevention And Mitigation:

A **zero trust security** system is a system that does not trust all users or entities, whether external or already internal, and constantly verifies their identity.

Continuous authentication, authorization and validation

Least privileged access

Comprehensive **monitoring** of all network activity

Regular vulnerability assessment, scheduled **backups**, **encryption** of data at rest and in transit, proper data setup, and uptime of systems and software can help prevent data breaches and reduce explosions when they occur.

But today, organizations can use certain data security management to prevent data breaches and minimize damage.

Organizations are using advanced **artificial intelligence** (AI) and automation to **counter threats** Technologies and responses such as **SOAR** (Security Orchestration, Automation and Response), **UEBA** (User and Entity Behavior Analysis), **EDR** (Endpoint Detection and Response), and **XDR** (Extended Detection) leverage AI and advanced analytics to find threats (even threats before it leads to data breaches) andallocate operational resources for faster. Training employees to recognize and avoid these attacks can reduce the risk of company data being compromised. Additionally, training employees to manage data properly can help prevent data conflicts and data breaches. Strong password management policies, password managers, two-factor authentication **(2FA)** or multi- factor authentication (MFA), single sign on (SSO), and other controls Identity and access management (IAM) technology can help organizations better protect themselves.

Data Breach of Verzion company

Introduction:

Verizon Communications Inc. is an **American communications company** that provides a variety of communications and entertainment services. The company was founded **in 1983** as **Bell Atlantic** and went through several mergers and acquisitions before changing its **name to Verizon** in **2000**. Headquartered in New York Cit,verizon has become the world's largest telecommunications company. Verizon operates in many areas such as wireless communications, telecommunications and media.The company is known for its wireless services, providing voice, data and messaging **services to millions of customers** in the United States. Verizon's wireless network is known for its breadth and reliability. Verizon continues to be a major player in the telecommunications industry, working to meet the daily communications needs of individuals, businesses and communities.

Data Breach:

In **March 2023**, information on **more than 7 million Verizon users** was published on the popular hacking forum Breached Forums. This information **includes contract information, device information** and **user passwords**.accounts were accessed by a third party during an attack that occurred on October 6 and 10. In total, approximately **250 prepaid wireless accounts** were **compromised during the attack.** During the attack, the last four digits of the customer's payment card were captured. While this doesn't allow the card to be used for other purchases, it does provide enough information for hackers to obtain additional accountdetails,**including names, phone numbers and billing addresses**Hackers can also perform **illegal actions** such as **SIM swapping**. This allows other devices to block messages or calls sent to the account owner, which may affect other accounts

In **May 2022**, a hacker livestreamed Verizon employees' internal contact information and other details, including names, ID numbers, phone numbers and email addresses. The **attackers** claimed they **used social engineering to gain access to internal systems** and then download files. Hackers demanded $250,000 to obtainprivateinformation.

In **July 2017**, Verizon admitted that the information of **6 million** Verizon customers was **leaked online**. The company said **misconfiguring** the cloud server allowed anyone to view the data. The information disclosed includes customer names,phonenumbersandPINs.

In **March 2016**, information emerged that a hack had exposed the contact information of **more than 1.5 million** Verizon Enterprise customers. The information was accessed through a **security breach** and later leaked to cybercrime forums. Hackers are offering customers' information for sale for prices ranging from $10,000 to $100,000. Additionally, the agency provided information about vulnerabilities associated with Verizon's website as an option for interested buyers.

Hacker access the data by performing **social engineering attack and SIM swapping**,through **security breach** and due to **misconfiguring** the cloud server.

Hacker Approached ways:

SocialEngineeringAttacks:

Social engineering is a **method** used by **criminals** to manipulate people into **rev ealing confidential information,** doing something**,** or making securityrelated m istakes**.** Techniques include phishing emails, **pretexts, baits,** quid pro quo offer s,andmore.

Example: It is a common scenario **for hackers to pose** as a **trusted person** to trick **others** into providing sensitive information or clicking on **the link is bad.**

Security Breach:

A security breach occurs when **an** unauthorized person **gains access** to confiden tial or sensitive information, a system, or a network. This **can** be **due to many r easons,**including**bugs,applications,**orhuman**error.**

Cause: A security breach can **be caused by poor operation, missing** passwor ds, **missing** software, **improper** security settings, insider threats, or other **factor s that are weak** in **the organization. Security infrastructure.**

SIM swapping

SIM swapping, also known as SIM swapping or SIM hijacking, is a cyber attack **in which** an attacker fraudulently **gains** control of **a** person's mobile phone nu mber. This attack involves using a mobile phone or service provider to associate the victim's phone number with a SIM card controlled by the attacker. Once the attacker takes control of the victim's phone number, he can use this number for various malicious purposes. Here's how SIM swapping usually works:

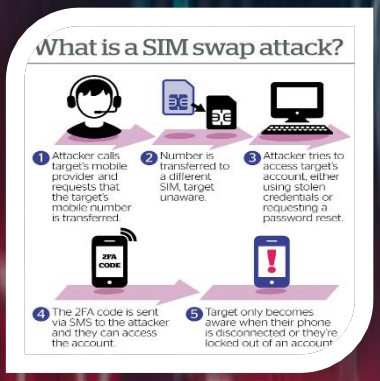

Fig2:Sim swapping process

Social Engineering:
Attackers often start by collecting victim information such as phone numbers, e mail address, and personal details.They may use a variety of social engineering t echniques (such as phishing) to trick victims or mobile phone users' support staf f into revealing sensitive information.

ContactMobileOperator:
The attacker contacts the victim's mobile operator and pretends to be the legitim ate owner of the account.They claim to have lost their phone or SIM card and as k to use the victim's phone number to replace the SIM card.

Authentication and Verification:
An attacker can use collected personal information to bypass security checks an d even leverage a support representative to assist with SIM swapping.

Getting a new SIM card:
After having the mobile phone user insert a new SIM card, the attackers use the victim's phone number to unlock the card.

Control:
The attacker can effectively control the victim's phone number by using a new S IM card.They can receive phone calls and text messages sent to victims, includi ng two-factor authentication codes sent by various services.

Abuse:
An attacker can use this exploit to gain access to the victim's account, bypass two-factor authentication, and lie.
SIM switching is a serious security issue, and individuals and organizations are advised to take precautions such as using other forms of two-factor authentication (such as authenticator apps), sharing personal information carefully, and notifying mobile phones if available. Incredible things. Mobile op erators are also encouraged to improve security measures to prevent unauthorize d SIM changes.

Action Categories:

Environmental															
Error	2	8	5	50	17	127	89	52	17	6	13	21	164	4	5	14
Hacking	31	12	27	95	50	251	175	201	123	17	58	227	248	31	88	46
Malware	37	19	31	94	31	86	107	138	114	23	35	216	210	30	124	56
Misuse	4	1	4	15	4	38	64	19	11	3	4	15	15		8	2
Physical	2		2	3		8	16	4	2	1	3	5	4	1	12	3
Social	11	5	13	48	14	70	46	80	62	2	28	78	79	10	43	16

Fig3:Action categories

Hacking: attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms.

Malware: any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent.

Error: anything done (or left undone) incorrectly or inadvertently

Social: employ deception, manipulation, intimidation, etc., to exploit the human element, or users, of information assets.

Misuse: use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended.

Physical: deliberate threats that involve proximity, possession, or force.

Environmental: not only includes natural events such as earthquakes and floods, but also hazards associated with the immediate environment or infrastructure in which assets are located.

Patterns of incident:

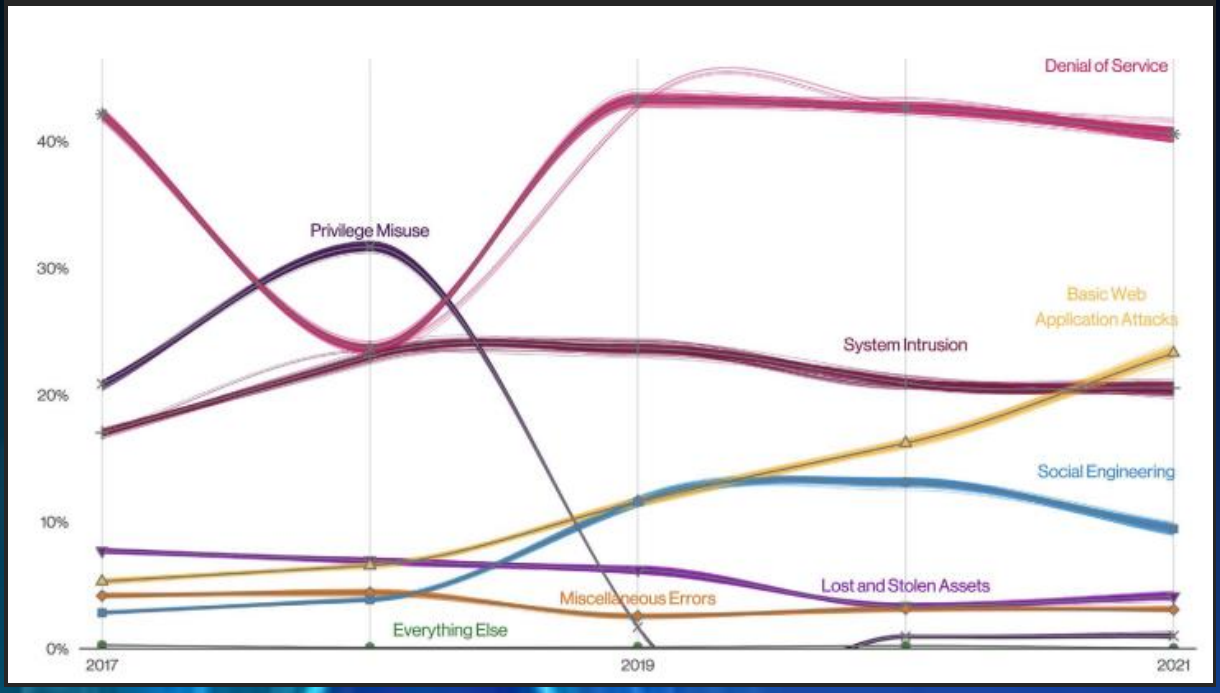

Fig4: Patterns over time in incidents

Basic Web Application Attacks These attacks are against a Web application, and after initial compromise, they do not have a large number of additional Actions. It is the "get in, get the data and get out" pattern.

Denial of Service Attacks intended to compromise the availability of networks and systems. This includes both network and application layer attacks.

Lost and Stolen Assets Incidents where an information asset went missing, whether through misplacement or malice.

Miscellaneous Errors Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.

Privilege Misuse Incidents predominantly driven by unapproved or malicious use of legitimate privileges.

Social Engineering A psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.

System Intrusion Complex attacks that leverage malware and/or hacking to achieve their objectives including deploying Ransomware.

Everything Else This "pattern" isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns. Like that container where you keep all the cables for electronics you don't own anymore: Just in case

Early Detection Techniques:

Breach sense platform is a commercial platform for organizations to **monitor and alter for potential data breaches**. BreachSense offer advanced features, threat intelligence, and support as part of their service packages. BreachSense typically operates as a web-based service that aggregates and analyzes data from various sources, including the dark web, to identify whether an individual or organization's sensitive information has been compromised.

Security Information and Systems Management (SIEM) Systems:

Examples: Splunk, LogRhythm, Elastic SIEM

Description: SIEM tools collect and analyze information collected from various systems and applications on the organization's network. They can help identify unusual patterns or activity that may indicate a security situation.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):

Examples: Snort, Suricata

Description: IDS monitors a network or activity for misconduct or security breach. IPS can also take steps to prevent threats. They can effectively detect and respond to unauthorized access or poor network connectivity.

Endpoint Detection and Response (EDR) Solutions:

Examples: CrowdStrike, Carbon Black, SentinelOne

Description: EDR solutions focus on the monitoring and response functions of a device (endpoint). They detect and mitigate threats such as malware, suspicious transactions, and unauthorized access to devices on the organization's network.

Vulnerability Scanning Tools:

Examples: Nessus, OpenVAS

Description: Regular system analysis and network vulnerabilities can help identify entry points for opposition. Addressing these issues proactively will reduce the risk of data theft.

Network Traffic Analysis (NTA) Tools:

Examples: Darktrace, Vectra AI, Cisco Stealthwatch

Description: NTA tools analyze network traffic patterns to identify unusual behavior or signs of violence. They can detect data anomalies or communication patterns that may indicate a breach.

Data Loss Prevention (DLP) Solutions:

Examples: Symantec Data Loss Prevention, McAfee Total Protection for DLP

Description: DLP tools help prevent unauthorized access and transfer of sensitive information. They can monitor and alert for possible data breaches by analyzing data in motion, at rest or in use.

Threat Intelligence Platforms:

Examples: ThreatConnect, Anomaly, Future Insights

Description: These platforms provide real-time information about threats, vulnerabilities, and attack patterns. Integrating threats into the security monitoring process increases the ability to identify and respond to vulnerabilities.

Data breach be split into two components - leads and indicators.

•Leads are server logs that indicate a security incident or an attack notification by a cybercriminal group.

•An indicator, as we discussed, is a factor that suggests a breach has either been experienced or is, in fact, happening in real-time.

Early indicators

Unusual network activity

Unauthorized data access attempts or unusual account activity

Unexpected database changes or missing files

Increased number of phishing emails to employees

Issue with system performance

Personnal advices to mitigate:

Be aware of Data Breach

Make everything up to date

Secure data by strong passwords

Monitor the data everytime by using official platforms and tools

Fix errors

Be aware of fraudulent links,attatchments,etc

Aware of SE attacks and ransomware attacks

Install secured firewalls and antivirus softwares

Secure physical devices

Conclusion:

By this I conclude that this investigation makes us to know complete analysis of Verizon company data breach incident and aware of data breach and their secure policies.This data breach leads to destroy the organizations reputation,heavy data loss,Financial loss,misuse of innocent people data and curroption of physical devices.

Conclude the report by summarizing the overall impact, the response efforts, and the commitment to preventing future breaches. Reiterate the dedication to security and continuous improvement of organizations.